经典重读

科技时代

KE JI SHI DAI

唐明 等/主编

黑客传奇

（下册）

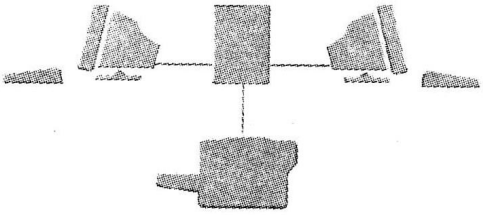
您，离不了的第三者——Internet!

远方出版社

经典重读

科技时代
黑客传奇(下册)

主编:唐明　等



远方出版社

责任编辑：王顺义
封面设计：杨　静

经典重读
科技时代
黑客传奇（下册）

主　　编	唐明　等
出　　版	远方出版社
社　　址	呼和浩特市乌兰察布东路 666 号
邮　　编	010010
发　　行	新华书店
印　　刷	北京兴达印刷有限公司
版　　次	2005 年 1 月第 1 版
印　　次	2005 年 1 月第 1 次印刷
开　　本	850×1168　1/32
印　　张	760
字　　数	4980 千
印　　数	5000
标准书号	ISBN 7-80723-005-3/I・3
总 定 价	1680.00 元
本册定价	20.00 元

远方版图书，版权所有，侵权必究。
远方版图书，印装错误请与印刷厂退换。

前　言

黑客到底是“明客”、“快客”、还是“害客”？

网络时代，黑客惊世骇俗的智力和行为引发了世界经济、军事、科技、个人生活各方面的震荡，本书为您提供一幅洞悉黑客神秘的智力杀拼的全景图像。

本套书出台的初衷是想通过大量事例向读者呈现一幅黑客全景画像，让读者通过感性材料来对黑客现象有一理性把握。在对日益引起人们关注的黑客现象做一全方位的扫描透视的同时，普及一些计算机和网络知识，希望能给读者一点小小的帮助。

值得声明的是，本套书在组稿过程中参

考了一些国内黑客文化研究和计算机犯罪方面的书籍，在此对作者表示感谢！

编　者

此为试读，需要完整PDF请访问：www.ertongbook.com

目 录

第六章　黑客帝国的无辜者：受黑的民用机构

通往电脑的路不止一条，所有的信息都应当是免费的。打破电脑集权，在电脑上创造艺术和美，计算机将使生活更美好。

——黑客道德准则

黑客们攻击政府网站是为了挑战权威，侵入银行网络是为了经济利益，与这些不同的是，黑客们对民用机构的入侵，体现了黑客的主张信息共享的精神以及他们的破坏心理，通过这种方式，他们觉得在某种程度上实现了自身的价值。

照客们对民用机构的入侵既不像入侵政府机构计算机网络那样引人注目，也不像入侵金融机构那样涉及巨额的资金，但是，黑客入侵民用机构对于当事者来说损失

还是巨大的。

一、网络安全,风雨飘摇

随着 INTERNET 的兴起,各种网站如雨后春笋般的兴起,以几何级数的速度增长,然而这个过程并没有伴随相应的安全措施,就我国的情况而言,我国 95% 的网络遭受过黑客入侵,我国的计算机网络发展迅速,导致安全性人才十分缺乏,网络安全方面的专家更是凤毛麟角,更可怕的是,我国网站普遍缺乏安全意识,网络管理员的理想就是保证系统正常运行,而严密完整的安全保障体制则普遍缺乏,从另一个角度看,网络安全防护的投资往往很大,专用软件的价格高得惊人,而国内网站往往运作资金不宽裕,不愿意把太多的钱投进看不见、摸不着的安全防护上,这些情况极大地妨碍了国内网站的安全防护工作。

国内黑客案风起云涌

近年来,我国的黑客也随着网络一起"茁壮成长""涌现"了不少黑客侵袭网络事件。

1998 年 4 月广州一名电脑“黑客”曾非法入侵中国公众多媒体通信网广州主机,酿成该主机系统管理失控 15 个小时的严重后果。该破坏计算机信息系统罪由广州市检察院向法院提起公诉。

此案的被告人吕薛文,男,24 岁,广州人。1997 年 4 月间,吕加入国内“黑客组织”,并在互联网中获得攻击与中国公众多媒体通讯网广州主机同类的计算机系统的方法。

1998 年 1 至 2 月间,吕在省中山图书馆多媒体阅览室外及其家中,利用手提电脑,盗用邹某某等人的账号使用一些非法账号上网活动,攻击中国公众多媒体通信网广州主机,成功入侵该主机系统后,取得该主机的最高权限,非法开设两个具有超级用户权限的账号以便其长期占有该系统的控制权。此后,多次非法入侵该主机,对该主机系统部分文件进行修改、增加、删除,造成该主机系统管理失控七个小时的严重后果。1998 年 3 月,此案由广州市公安局侦破。

1999 年 1 月,内蒙古警方查获一个 13 岁黑客非法侵入一六九多媒体信息港案件。这位就学于呼和浩特市某中学的二年级学生,在 1998 年 10 月初,通过破译口令,修改口令,非法取得了对呼市多媒体通信公司系统管理员工作账户的控制权。据悉,系统管理员的这个工作

账户,具有对数据库文件进行某些重要处理的高级权限,如果非法侵入者抱有不良目的,将会造成很严重后果。这位少年的非法攻击行为已触犯了国家法律,但由于其未满14周岁,警方根据有关法律做出责令其家长加以管教的决定。

1999年1月北京市警方对外宣布,中国新刑法实施以来,京城首例利用计算机进行犯罪的案件已被北京市公安局朝阳分局破获,犯罪嫌疑人张文明已被抓获归案。1998年12月31日,北京无忧电脑软件开发公司报案称:公司在1998年底开发的一级A类计算机等级考试DOS学习软件中发现病毒。接报案后,朝阳公安分局立即成立了由专业技术人员参与的专案组,迅速展开全面调查。据了解,无忧公司于1998年底开发了两套计算机等级考试软件,并将软件复制生产了2万套,目前已售出1.6万套。公司有关人员介绍说,两套计算机等级考试软件的客户主要是学校,经初步测试,已发现的病毒为"逻辑炸弹"病毒,它将于1999年3月27日和以后的每月27日爆发,届时,只要运行该学习软件,病毒将自动转化为EXE文件,导致硬盘文件被删除,并破坏分区,从而给用户造成不可估量的损失。据估算,由于两套学习软件染上病毒,不仅给公司的声誉造成了恶劣影响,而且由此造成的直接经济损失达150余万元人民币。为及时侦

此为试读,需要完整PDF请访问: www.ertongbook.com

破这一高科技犯罪案件,北京警方多次走访有关人员,收集了大量的证据材料,并找到了制作计算机病毒的代码和有害程序的原文打印件,初步确认原该公司开发部主管张文明有重大嫌疑。1999 年 1 月 10 日,北京警方依法传唤了张文明,经审讯,张文明终于供认:因与公司领导发生矛盾,为图报复而利用工作之便,将一个外国病毒修改逻辑植入公司开发的一级 A 类计算机等级考试 DOS 学习软件中。目前,此案仍在进一步审理之中。据了解,无忧公司售出的带有病毒的学习软件大部分已被收回。

1999 年 6 月 28 日深夜 11 时许,成都一信息中心的网络上竟然骤响阴森恐怖的"午夜凶铃",并致使该网络电子邮件系统完全被"坏死了"。四川省公安厅计算机安全监察处接到报案后,立即展开侦破。警方很快查明该破坏性恐怖电子邮件来源于四川广播电视大学的代理服务器。在充分的证据和强大的政策攻心压力下,"黑客刘某某终于现出原形,7 月三日非法侵入网络 4 次,7 月 15 日 12 时再次侵入,时间长达 28 分钟。

根据上述情况,专案人员分析此案板有可能是这个公司内部人员或曾经在此公司工作过的人员所为。据了解,原来在这家公司主管计算机系统维护编程,3 月份跳槽到另一家公司的计算机系统管理员王波,存在重大作

案嫌疑。后经缜密调查,发现了王波的作案线索。7月19日,王波供认了自己利用现所在公司办公室的电脑,先后5次侵入太平洋保险公司网络,修改、删除寿险信息系统数据的犯罪事实。据他交代,他侵入网络的动机主要是听人说原来公司经理认为他的技术不行,有的同事还说他工作干得不好,于是心理上感到不平衡,想借此办法显示一下自己的技术能力,并进行报复,目前,王波已经被刑事拘留。

2000年2月,大连市公安局破获一起"黑客"攻击计算机信息系统案。

2月1日下午3时左右,大连市公安局计算机安全监察部门接到大连一家网络服务公司报案,这家公司的计算机信息系统正在遭来访用户的攻击,计算机信息系统受到破坏,疑是"黑客"所为。大连市公安局计算机安全监察人员接到报案后立即赶到现场进行侦破,经过反复技术监测,下午5时,终于捕捉到"黑客"踪迹。经过进一步工作,终于确定了"黑客"作案现场,当晚8时,这家公司计算机邮件服务系统崩溃,造成严重经济损失。

2月2日"黑客"被公安人员传讯,并依法扣押了作案使用的计算机,经讯问,"黑客"谢某系国内某名牌大学毕业的学生,现在大连一家单位任副科长。谢某爱好计算机,他采用先在网上下载"黑客"程序,然后,用这家

计算机网邮件服务器来运行“黑客”程序。这名“黑客”承认其违法事实,但他称攻击这家计算机信息系统的目的是想在春节假期利用这家计算机信息系统上网。

1999 年,我国共破获黑客案百余起,电脑黑客案的猛增已引起社会各界的关注,统计数据表明,近年来,利用计算机网络进行的各类违法行为在中国以每年 30% 的速度递增,黑客的攻击方法已超过计算机病毒的种类,总数近千种,公安部官员估计,目前已发现的黑客攻击案约占总数 15%,多数事件由于没有造成严重危害或商家不愿透露而未被曝光,中国社会科学院国家信息安全重点实验室赵战生以为,中国的电子信息网络建设处于初级阶段,网络安全系统脆弱,而“监守自盗”式的内部攻击对网络安全构成了更大的威胁。

1998 年 11 月在伦敦举行的计算机安全会议上有一条出人意料的发现,对公司网络构成更大威胁的,不是公司外面的人员,而是内部雇员。

此次会议的组织单位 DiligenceIntormationSecurity 宣布,在公司的安全检查故障中,有 70% 乃内部员工所为,其中相当一部分是担心裁员被裁下的员工。最近就有这样的案例:一名员工在发现自己的名字从薪水册中删掉后,就用黑客程序捣毁了公司的中枢数据库。在国内,在福州,新近更有作为电子阅览室管理员的杨峰侵入所在

图书馆计算机查询系统网络,导致该系统两度关闭。杨峰时年39岁,为中银奥力威集团教育行业部职员,半年前借调到福建省图书馆电子阅览室当管理员。杨峰平时在网上以侠客自居。9月底,他用从一帖子上看到的方法,盗用他人账号,在家中通过互联网两次侵入省图书馆计算机查询系统网络,并改动了主页内容。(写上"大眼睛女孩的名字我还不知道呢?"等字句,并自由链接"网上城市"等其他站点)省图书馆服务器因此两度关闭。为防止信息入侵,该系统被迫在此后关机6天。现在杨峰已被捉拿归案。

据国外的报道,大部分的网络安全不堪一击。一位安全专家说,他的公司在过去一年半中应邀为50个站点测试安全性。结果都以非常简单的办法轻松闯入。无一例外,国内的情况也差不多,金华信息技术公司对上海、深圳等地几十家证券机构进行模拟黑客攻击测度,结果发现它们的电脑普遍存在漏洞,在一些机构,测试者仅用一台笔记本电脑,由一条缆线接入其电脑网络的任何一点,就可以在一分钟之内侵入网络核心,随便划转资金和更改信息,由于网络是新事物,目前对网络的立法还没有跟上,我国尚无明确法规来处罚那些造成危害或危害较轻的黑客,为确保网络安全,中国已经在《刑法》中增加了惩治计算机犯罪的条款,并制定了《计算机信息系统

安全保护条例》和《计算机信息系统安全专用产品检测和销售许可证管理办法》等法规，自 1997 年在扬州抓获中国第一个电脑黑客以后，司法部门已先后将多名黑客送上法庭，除了法律措施，相应的技术保障也必不可少，我国的绝大多数计算机软件硬件都是从国外进口的，产品的安全级别也是国外鉴定的，这种建立在别人技术上的安全是不可靠的，我国应花大力气研制自主版权的电脑密码，改变电脑加密系统依赖进口的局面。广东省经济比较发达，因此网络普及率也比较高，这方面的工作就做得比其他地方好些，广东省公安厅计算机安全监督办公室主任江某说，广东警方对于计算机安全防范工作是敏感的、充分的，截止 1999 年底，广东省政府及商业网站暂无因遭受黑客攻击遭受巨大损失。江主任建议所有网络用户在技术可行的范围内尽量采用国产计算机软件及安全产品，这是防止国外黑客攻击最长远而有效的办法，值得注意的是，广东警方已发现某些进口的计算机安全产品以远程维护为借口故意留下安全漏洞，为其幕后公司或组织留下信息殖民的人口，因此，积极发展民族计算机产业，在技术上不受制于人，才是防止国外黑客攻击的长远之计。

不设防的系统

网络安全问题日益突显出安全的重要性,但是现在最危险的不是黑客,而是人们对计算机安全的观念非常淡薄,许多计算机系统几乎是"不设防"。"黑客"经常被描写成是一些天资聪明的孩子,事实并非如此,那些遭到袭击的计算机系统往往是只有极差的防御措施。侵入这些系统就如打劫一个没有关门的银行保险库那样易如反掌,这并不需要高深的技术。许多情况下,他们通过一些现成计算机程序和工具包自动找寻路径,根本不需要什么技能。比如有个叫"ROOTDIT"的程序,它可以侵入到一台计算机而隐匿所有的入侵踪迹。使用这种程序只需在提示将下输入一个单词"MAKE"。美国计算机紧急情况反应小组协作中心的专家认为,这些少年"黑客"的神童形象是假的,而制造这种假象将十分危险,因为这将误导人们忽视可能是最大的计算机安全问题——计算机系统的脆弱性。简言之,许多人并不懂得如何使用合理的安全级别来管理计算机网络。举个例子说,几个月前,Jim(吉姆)买了台预装有 Windows95 的笔记本电脑。Jim 将他的电脑联上了他公司的内部网,同时他又在 Internet 上下载了一个非常流行的游戏软件"DOOM"。因为他的

此为试读,需要完整PDF请访问: www.ertongbook.com